

загальному випадку мають дві рівноцінних панелі для списку файлів, дерева каталогів і т.п.

На даний момент дуже широке розповсюдження отримали пристрої, які працюють під операційною системою Apple iOS. Apple iOS – мобільна операційна система, розроблена компанією Apple на основі Mac OS X для смартфонів iPhone, медіаплеєрів iPod Touch і планшетних комп'ютерів iPad. Була випущена 29 червня 2007 року, з тих пор регулярно обновляється. Входить у сімейство операційних систем Apple OS X, до якого також відноситься й операційна для настільних комп'ютерів – Mac OS X. Операційна система Apple iOS також працює на Apple TV, але з користувальницьким інтерфейсом, що відрізняється.

Розробка програмного забезпечення захисту інформації у мережі на основі інфраструктури відкритих розподілених ключів

А.В. Підгорна, студент,

О.А.Смірнов, доцент, канд. техн. наук

Є.В. Мелешко, ст. викладач, канд. техн. наук

Кіровоградський національний технічний університет

Сучасна інформаційна взаємодія вимагає високої швидкості передачі даних, що приводить до збільшення частки інформаційних технологій, використовуваних у цій взаємодії. До складу переданих даних неминуче включається все більш важлива інформація (персональні дані, відомості, що містять комерційну таємницю, і багато чого іншого), що передається через незахищену мережу Інтернет. Для забезпечення цілісності даних, їхньої автентичності, юридичній значимості й неможливості відмови від авторства використовується асиметрична криптографія, що лягла в основу інфраструктури відкритих ключів (PKI).

Метою роботи є розробка програмного забезпечення захисту інформації у мережі на основі інфраструктури відкритих розподілених ключів.

Об'єкт дослідження – процес захисту інформації у мережі на основі інфраструктури відкритих розподілених ключів.

Предмет дослідження – програмне забезпечення продуктів, що відносяться до інфраструктури відкритих ключів (на прикладі S/MIME), а також методи аналізу їхньої споживчої якості.

Методи дослідження. Для рішення поставлених задач у роботі використовувалася теорія інформаційних систем і статистичного аналізу. Також використовувалися імовірнісні методи визначення якості складних систем і методи аналізу предметної області. Теоретичною основою дослідження є наукові праці українських і закордонних вчених по теорії вибору й прийняття рішень, математичному моделюванню.

Наукова новизна:

– складено перелік функціональних операцій для інфраструктури відкритих ключів, що відрізняється деталізацією елементарних операцій до рівня мережних

протоколів і що дозволяє порівнювати інфраструктури відкритих ключів за критерієм функціональної повноти;

- розроблено метод розрахунку трудомісткості виконання групи функціональних операцій в РКІ, що відрізняється використанням частоти звертання до функціональних операцій і статистичних характеристик, виконання кожної елементарної операції, і що дозволяє оцінювати витрати часу на виконання групи функціональних операцій і їхніх транзакцій при заданій імовірності;

- розроблено метод визначення ефективного числа вузлів у РКІ-системі, що відрізняється застосуванням моделі масового обслуговування, побудованої на основі програмного кластера РКІ-системи, і, що дозволяє шляхом послідовного перебору для області припустимих рішень знайти необхідне число вузлів у системі для досягнення заданої пропускну здатності;

- сформовано профіль інфраструктури відкритих ключів, що включає в себе перелік функціональних операцій і час їхнього виконання, що відрізняється використанням тимчасових характеристик і дозволяє проводити порівняльний аналіз РКІ-систем і визначати рекомендації з підвищення їхньої ефективності.

Практична значимість роботи визначається тим, що основні положення, виводи, рекомендації, моделі, методи й алгоритми можуть використовуватися підприємствами й організаціями будь-якої структури, відомчої приналежності й форми власності для оцінки споживчої якості інформаційних систем, що використовують інфраструктуру відкритих ключів.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів приватним результатам, наведеним у науковій літературі.

Програмне забезпечення менеджера завантажень

Д.Ю. Беліч, студент,

О.П. Доренський, викладач

Кіровоградський національний технічний університет

Менеджером завантажень (download manager) є комп'ютерна програма, призначена для завантаження файлів на комп'ютер (робочу станцію) з Інтернету або локальної мережі. Менеджери download значно полегшують процес завантаження файлів із серверів через мережу Інтернет на локальний комп'ютер.

Дослідження показали, що на українському ринку програмного забезпечення (ПЗ) download-менеджери представлені в недостатній мірі. Тому розробка програмного забезпечення download-менеджера є актуальною задачею.

Аналіз існуючого програмного забезпечення показав, що серед найбільш затребуваних опцій менеджерів завантаження можна відзначити: убудований FTP-клієнт, можливість перегляду Zip-архівів перед завантаженням, одержання розміру файлів до початку завантаження, перевірка й відновлення архівів, установка пріоритетів для завантажень, робота з командним рядком, завантаження HTML-сторінок із зображеннями, розширені можливості за допомогою плагінів та ін. Тому зазначені функції необхідно врахувати під час розробки ПЗ. В доповіді наводиться